Consumer security behaviors and trust following a data breach

Shelby R. Curtis, Jessica Rose Carre and Daniel Nelson Jones
Department of Psychology, University of Texas at El Paso, El Paso, Texas, USA

Abstract

Purpose – The purpose of this study was to determine how security statement certainty (overconfident, underconfident and realistic) and behavioral intentions of potential consumers impact the perceptions of companies in the presence or absence of a past security breach.

Design/methodology/approach – The study exposed participants to three types of security statements and randomly assigned them to the presence or absence of a previous breach. Participants then evaluated the company and generated a hypothetical password for that company.

Findings – This study found that the presence or absence of a previous breach had a large impact on company perceptions, but a minimal impact on behavioral intentions to be personally more secure.

Research limitations/implications – The authors found that the presence or absence of a previous breach had a large impact on company perceptions, but minimal impact on behavioral intentions to be personally more secure.

Practical implications – Companies need to be cautious about how much confidence they convey to consumers. Companies should not rely on consumers engaging in secure online practices, even following a breach.

Social implications – Companies need to communicate personal security behaviors to consumers in a way that still instills confidence in the company but encourages personal responsibility.

Originality/value – The confidence of company security statements and presence of a previous breach were examined for their impact on company perception and a novel dependent variable of password complexity.

Keywords Cyber security, Security statements

Paper type Research paper

Introduction

Data breaches are damaging to a company's reputation and revenue, specifically those in which unauthorized access to confidential information occurs (Acquisti *et al.*, 2006; Campbell *et al.*, 2003). Although companies may under-report, or refuse to report, the financial impact of a security breach, observational research and event studies find that impacted companies experience an immediate drop of 5.6 per cent in stock shares. Further, companies can experience financial loss between $17 and $28m per incident (Garg *et al.*, 2003; Morse *et al.*, 2011). These incidents have also been found to lower consumer trust and intentions of shopping online, especially among older adults (Chakraborty *et al.*, 2016). In non-online–based companies, such as hotels, breaches also have a negative impact on consumer perception, satisfaction and intent to revisit (Berezina *et al.*, 2012). However, it is important to note that the fault of security breaches is not always with the company. For example, research by Berendt *et al.* (2005) found that although online users may indicate that they expect and prefer specific privacy behaviors and systems, they often do not act in accordance with these stated preferences.

In spite of their potential contribution to company susceptibilities to data breaches, individuals often perceive that the onus of responsibility for data security lies solely with an

Managerial Auditing Journal
© Emerald Publishing Limited
0268-6902
DOI 10.1108/MAJ-11-2017-1692

online company or vendor. Vendors that store personal or financial information of consumers have pushed for better online security and reputations for security, which may have had the unintended consequence of false security for consumers (Carré *et al.*, 2018). Further, Carré *et al.* found that following a data breach, individuals are more likely to repudiate the quality of a company, specifically among selfish personality types. However, individuals often engage in behaviors that can put online companies at risk for hacking and breaches. Specifically, users perceive that engagement in secure behaviors is an inconvenience and that many messages about security awareness do not result in behavioral changes (Ng *et al.*, 2009).

An unwillingness to change may be driven by a lack of knowledge. For example, although internet users feel strongly about privacy and security, many lack the knowledge to behave in ways that protect themselves (Miyazaki and Fernandez, 2001). However, even among those who do have the ability and/or knowledge, many individuals simply do not engage in basic (although, time-consuming) activities that would prevent security being compromised, such as disabling cookies, reading terms of service agreements for using private information and using secure searching shells (Papacharissi and Fernback, 2005). Recent research has even gone so far to suggest that companies should entirely omit reliance on user security practices from their expectations and analyses of their security systems (Kang *et al.*, 2015). Nevertheless, even if the cultural perceptions and prevailing norms are that the online company bears the highest minimum burden of data security, security maintenance can still be enhanced by consumers engaging in a set of simple behaviors.

One of the most vulnerable aspects of security, which relies on consumer behavior, is that of password protection and strength. Security experts have been known to state that a system is "only as secure as the weakest password" (Schneier, 2011, p. 139). Individuals have been found to be relatively susceptible to socially engineered attacks to gain access to passwords, such as phishing attempts via email (Curtis *et al.*, 2017), and may often keep passwords written down, reuse them across websites, or even share them with others (Stanton *et al.*, 2005). With respect to password complexity, most individuals who are given a character minimum tend to stick to that minimum, rather than add additional complexity that would make discovery of the password more difficult (Proctor *et al.*, 2002; Summers and Bosworth, 2004). Password cracking algorithms, such as the Weir-calculator, can run over 50 trillion password guesses within 24 hours. Using data collected from online participants, Kelley *et al.* (2012) were able to guess over 50 per cent of user-generated passwords within this time when minimum requirements were basic. In a study conducted by Cazier and Medlin (2006), 28.5 per cent of passwords collected from an e-business site were cracked in less than one minute. Further, consumers often re-use passwords across multiple accounts, which highly increases the risk of discovery and hacker infiltration (Ives *et al.*, 2004). Thankfully, there are methods to increase the complexity of user passwords; such as requiring stronger minimum character requirements. Although users show frustration when forced to create more complex passwords, they also tend to believe they are now more secure (Shay *et al.*, 2010). Another is to incorporate password strength meters into a company website. These meters give real-time feedback as to the strength of the user-generated password and have been shown to increase password complexity (Egelman *et al.*, 2013; Ur *et al.*, 2012).

The studies on password complexity discussed above have only researched password generation for companies regardless of breach history or security statements. However, a recently unexplored area of research is in how individuals may behave when they know a security breach has occurred for an online company in the past. Although Carré and colleagues (this issue) demonstrated that a security breach will compromise the perceived

quality of a company, it is yet unknown whether this compromise will translate into increased security behaviors on the part of the consumer.

Overcoming reticence to go online with financial information

Many companies have pushed for online security because of the profit margins associated with e-commerce. In the persuasion literature, there are (generally speaking) two forces that drive an individual towards action: approach and avoidance (Knowles and Riner, 2007). Thus, one strategy to draw users to companies is to emphasize the benefits and gains of e-commerce, while another is to reduce anxiety about security and costs through security statements. However, when it comes to communicating their confidence in the security of a consumer's information, slight differences in the wording of security statements may affect perceived trust and intentions. For example, a perceived guarantee of online security may create apathy on the part of consumers when it comes to their own security habits. In contrast, companies with too weak of a security statement may be perceived as untrustworthy. Thus, there may be an incentive for companies to remain strong but realistic in their security capabilities.

Another issue to consider is how a security breach may impact future perceptions of a company's security statement. If a statement is perceived as overly confident, it is possible that some individuals will hold a company more responsible for breaches that may occur. Thus, overconfident companies who have been breached may be perceived as less trustworthy and riskier to do business with. However, it is also possible that the manipulation of security statements may have little impact on a company's perception. For example, Metzger (2006) reported that only company reputation, not privacy assurances, impacted consumer trust. Thus, the presence of a security breach, regardless of security statement, maybe the only key aspect in influencing consumer trust and security behaviors. This study aims to examine several potentially key interactions that may emerge between statement certainty and presence of a previous breach that may impact perceptions of the company and password security.

Summary and hypotheses

Companies provide assurances to consumers about online security. Such assurances are not only evidence of ethical responsibility but also a vehicle to encourage high volume internet revenue. However, companies may want to be careful about communicating too much confidence in their own ability to keep information secure. When this security is compromised, such confidence may backfire. Further, individuals given too much assurance of security may resort to lackluster self-protective behaviors. In this study, we actively manipulate security statements made by companies as well as the presence or absence of a past security breach in order to analyze their effects on consumer trust and intended security behaviors.

We expect main effects for both the presence of a security breach and the level of confidence in a company's security statement. Specifically, we hypothesize that companies who have experienced a security breach will be perceived as less trustworthy and elicit higher vigilance of security behaviors than companies who have not been breached. Further, we hypothesize that companies with under confident security statements should be perceived and responded to in similar ways, regardless of the presence of a security breach. Finally, we also predict interactions between these variables such that individuals exposed to a company's overconfident security statement, who are then made aware of a security breach, will hold that company in lowest regard. This overconfident-breach condition

should also produce concern on the part of consumers, leading to increased password complexity and higher reports of intended security behaviors.

Methods

Participants

A power analysis was conducted using G*Power 3.1. Anticipating a medium effect size ($f = 0.25$) for a 3 × 2 design at a power level of 0.80, a minimum sample size of 211 was recommended. Data was originally collected from 285 individuals through Amazon's Mechanical Turk. Participants were excluded if they did not progress far enough into the survey to see any of the manipulations and complete any dependent variable measures. 24 participants were excluded from analysis for this reason. An additional 19 participants were excluded for failing an attention check in the survey. Specifically, this attention check said, "I will answer 'always' to this question" After exclusions, a total of 241 participants remained for analysis. 61.8 per cent of participants were female, with a mean age of 35.85 (SD = 11.63). Participants were primarily white (70.7 per cent) and heterosexual (82.2 per cent). We also asked for information about average income and education. Reports of income were pretty varied, with approximately 85 per cent of participants making less than $75,000, but evenly spread within that range. Around 49.6 per cent of participants reported having at least a Bachelor's degree, and only one participant reported having never graduated high school. Nearly 60 per cent of participants indicated that they usually spend more than four hours per day on the internet.

Procedure

Participants were recruited from Amazon's Mechanical Turk, a reliable source of representative participant data (Buhrmester *et al.*, 2011), for a study on online consumer perceptions. Once directed to the online survey software, participants filled out initial demographic information and questions about general internet use. Next, all subjects were given the following information about a fictitious company:

> Company X is an online and in-store retailer that offers a variety of products and services for purchase. Imagine you have just signed up for this Company's premium credit card, offering great rewards and minimal fees. As a credit card holder of Company X, this company has access to a variety of your personal and financial details, including your address, purchase history, marital status, travel history and primary bank account information.

After reading this statement, participants were randomly assigned to one of six conditions where both the security statement of Company X and the presence or absence of a security breach were manipulated. First, participants read a security statement from Company X that varied in its degree of confidence (overconfident, realistic and underconfident). Next, participants were informed that an external security rating website either had records of no prior security breaches of Company X or that a breach had occurred in the past month. Complete text of these statements can be found in Table I.

Once participants completed reading their randomly assigned information about Company X, they were asked to generate a password that they would use for online access to their account information with Company X. The only password requirements given were that it must be a minimum of 6 characters and that, for security purposes, it should be a password they have never previously used. Subjects then filled out two questionnaires as dependent variable measures of security behavior intentions and perceived risk and trust in Company X. More detailed information on these questionnaires can be found in the "Materials" section.

Security breach	*An external security rating website has provided the following statement regarding Company X's security history*
Breach occurred	Last month, a cyber security breach occurred. An unauthorized access took place, and, while damage is still being assessed, there is a possibility that personal and financial user information was compromised
Breach did not occur	Since the creation of Company X, no cyber security breaches have ever occurred
Company X security statement	*The following Security Statement can be found on Company X's website*
Overconfident security statement	Security is our top priority. Be assured that our website is the safest around due to our top-notch cyber security teams. It is impossible for your information to be compromised when you work with us
Realistic security statement	We strive to provide you with the most secure network possible by partnering with the leading cyber-security firms. The privacy and protection of your information are extremely important to us
Underconfident security statement	The security of your information is important to us. We try our best with the resources we have to uphold your privacy and protection

Table I. Complete text of prompts per condition

The final section of the survey once again randomly assigned participants to a condition where a security breach either did or did not occur. However, this time, participants were asked to choose, based on all three Company security statements, with which Company they would like to do business. To assess and confirm the perception of the security statements as "overconfident", "realistic" and "underconfident", participants also had the opportunity to describe why they chose the Company they did.

Materials

Modified Security Behavior Intentions Scale. To assess the degree to which participants intended to engage in risky security behaviors when using the website and credit card of Company X, participants were asked a modified subset of the initial questions from the Security Behavior Intentions Scale (SeBIS; Egelman and Peer, 2015). Because the original items in the SeBIS were intended for general security behaviors and we hoped to identify intentions specific to Company X, some questions required slight modifications for inclusion. Further, other questions, such as those about software updates and general device security, were not applicable to online security behaviors and credit card use. The modified SeBIS administered in this study consisted of 12 intention questions and an additional three filler questions asking about prospective engagement with and recommendation of Company X. Items were responded to using a 5-point Likert-type scale that ranged from 1 (*Never*) to 5 (*Always*). The complete list of items can be found in Table II. The reliability of the scale, as measured by Cronbach's alpha, was good ($\alpha = 0.81$). No factor structure was anticipated; therefore, the 12-item scale was averaged to form a composite variable of intended behavior. Higher scores on this composite variable are indicative of less secure behaviors.

Trust and Perceptions of Company X. A 10-item measure was used to assess trust and perceptions of risk of Company X. These questions were answered using a five-point Likert-type scale that ranged from 1(Strongly Disagree) to 5(Strongly Agree). Some of these questions were adapted from the survey questionnaire used by Kim *et al.* (2010) to assess perceived trust and risk. The reliability of the 10-item measure was excellent ($\alpha = 0.94$), and the exact items can be found in Table II. Higher scores on the composite variable generated from this scale are indicative of greater trust and perceived security in Company X.

Security behavior intentions scale (modified from Egelman and Peer, 2015)	Mean (SD)
I would submit information to the website without first verifying that it will be sent securely (e.g. SSL, https://, a lock icon)	2.05 (1.29)
When using public WiFi, I would visit this website	1.91 (1.16)
I would have my internet browser remember my password for this account	2.23 (1.36)
I would share my password if a friend or family member needed access to my account	1.76 (1.16)
I would frequently check my financial account for fraudulent charges (R)	3.65 (1.26)
I would save the information for this credit card on other online shopping websites	2.01 (1.25)
I wouldn't change my password unless the website told me to	2.60 (1.40)
I would download and use this company's app on my phone to access my secure account information	2.45 (1.34)
If I were to receive a suspicious email from this company, I would phone the company to make sure the e-mail is accurate (R)	3.46 (1.50)
If I discover a security problem, I would continue what I was doing because I assume the company will fix it	1.82 (1.11)
When accessing this website, I would use my own privacy software, "private browsing", or "incognito mode" (R)	3.00 (1.39)
I would access my account on other people's devices	1.62 (1.06)
Trust and perceptions of Company X	
I think it is highly unlikely that an authorized third party would be able to access my personal information through Company X	2.89 (1.21)
I think it is highly unlikely that an authorized third party would be able to access my credit card information through Company X	2.85 (1.28)
I believe that transactions conducted through Company X's website are securely protected	3.25 (1.16)
I believe that Company X is invested in the security and protection of my information	3.34 (1.16)
I would trust Company X to not release my personal information to any other companies or organizations	3.20 (1.25)
I perceive Company X as secure	3.17 (1.19)
I trust the security statement made by Company X	3.18 (1.18)
The security statement made by Company X makes me feel like my information is safe	3.13 (1.18)
I would trust Company X to have access to my personal information	3.07 (1.20)
I do not fear hacker invasions into Company X	2.56 (1.18)

Table II.
Dependent variable measures of security behavior intentions and trust/perception of company X

Results

Table III shows the overall correlations and descriptive statistics of the composite scores of the dependent variables: security behavior intentions, trust in Company X and password complexity. Older participants reported significantly more secure behavior intentions, and more daily internet use was indicative of slightly more complex passwords. Independent samples T-tests were also conducted to compare participant gender. The only significant difference between gender was that females reported more intentions of engaging in secure online behaviors than males [$t(238) = 2.29$, $p = 0.023$].

	Mean (SD)	Skew (Kurtosis)	1	2	3	4	5
Security Intentions Scale	2.19 (0.71)	0.30 (−0.64)	–				
Trust Scale	3.06 (0.97)	−0.43 (−0.34)	0.341***	–			
Password complexity	13.19 (35.60)	0.56 (−0.49)	−0.168**	−0.065	–		
Age	35.85 (11.63)	0.95 (0.14)	−0.189**	−0.012	−0.013	–	
Hours of daily internet use	4.25 (1.03)	−1.08 (−0.10)	−0.057	−0.027	0.141*	−0.073	–

Notes: *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$

Table III.
Correlations and descriptive statistics of dependent variables and demographics (N = 241)

Password complexity was identified through two main approaches. Currently, most advanced computer algorithms use a metric called "guessability", or the time needed for an algorithm to crack a password, as an indication of overall password strength (Weir *et al.*, 2010). These algorithms are often utilized to some degree in online "password meters" that analyze different patterns of the proposed password and return a qualitative judgment of the password (e.g. very weak; fair; strong; see de Carnavalet and Mannan, 2014). These meters may vary in regards to their cutoffs for different outputs of strength but generally use similar variables to compute their score. Some of these include length, character variability, keyboard sequence patterns and redundancy. Thus, we utilized a common password meter website: "yetanotherpasswordmeter.com", to generate a continuous metric of password strength. The range of password complexity in our sample was from −51 (123456) to 118 (E73#sj#DK9EgH*gUbKcR), with a score of 13.19 being the average. While 13.19 is considered a "weak" score according to the password meter, it was not unexpected considering that the most common types of passwords chosen by users have been found to be relatively susceptible to password cracking algorithms, with average lengths of 6-8 characters and monocharacteristic passwords (i.e. just alphabetic; Zviran and Haga, 1999).

To verify the accuracy of the password meter, we also used two proxy interactive characteristics to determine complexity: the total number of characters (range: 6-30) and the total number of different character types used (range 1-4; uppercase alphabet, lower case alphabet, numbers and ASCII/special characters). We then multiplied these two variables to create a single "password complexity" variable. This variable had a correlation with the password meter score of $r = 0.93$. The strength of this correlation indicates that the score generated by the password meter is an accurate representation of password strength and complexity using a continuous metric. Thus, all analyses concerning passwords only used the score generated by the password meter.

Two-way ANOVAs were used to analyze the effects of the security statement manipulation and presence of a past security breach on the dependent variables of intended security behavior, trust in Company X and generated password complexity. For intended security behavior, the main effect of breach was non-significant, $F(1, 235) = 1.023$, $p = 0.313$. Thus, the presence or absence of a security breach did not seem to impact participants' reports of their intended security behavior. However, the main effect for security statement was marginally significant, $F(2, 235) = 3.004$, $p = 0.051$, partial $\eta^2 = 0.025$, such that individuals in the "Overconfident" ($M = 2.24$, $SD = 0.73$) and "Under confident" conditions ($M = 2.31$, $SD = 0.67$) indicated they would engage in riskier online behaviors than those in the "Realistic" condition ($M = 2.04$, $SD = 0.71$). The interaction effect was non-significant, $F(2, 235) = 1.140$, $p = 0.322$.

A different pattern of results was found when the variable of interest was trust in Company X. For this analysis, the main effect for security statement was non-significant, $F(2, 235) = 0.462$, $p = 0.631$, but the main effect for breach was significant, $F(1, 235) = 26.588$, $p < 0.001$, partial $\eta^2 = 0.102$. People reported greater trust in the company when no breach had ever been reported ($M = 3.35$, $SD = 0.86$) compared to when a breach had occurred in the past month ($M = 2.74$, $SD = 1.00$). Once again, the interaction effect was non-significant, $F(2, 235) = 0.869$, $p = 0.421$. The final two-way ANOVA used password complexity as the dependent variable. Surprisingly, none of the effects in this model were significant. The main effect for breach was non-significant, $F(1, 233) = 0.015$, $p = 0.902$, the main effect for type was also non-significant, $F(2, 233) = 0.390$, $p = 0.677$ and the interaction effect was non-significant, $F(2, 233) = 1.660$, $p = 0.192$.

The final analysis conducted used a multiway contingency table to investigate whether the presence or absence of a security breach impacted the company and security statement

participants were likely to choose. Results indicated a marginally significant relationship between these variables, $G^2(2) = 5.738$, $p = 0.057$. Specific counts of the observed and expected values for each cell can be found in Table IV. Emerging patterns suggest that in the condition in which a security breach has never occurred, participants choose the overconfident company with higher than expected frequencies and the underconfident company with lower than expected frequencies. When a security breach has occurred, the pattern is switched, such that participants choose the underconfident company with higher than expected frequencies and the overconfident company with lower than expected frequencies.

Discussion

We explored the impact of security statement strength (overconfident, underconfident and realistic) and the presence of a security breach on perceptions of companies and intended and actual security behaviors. Our first hypothesis: that companies who have experienced a security breach will be perceived as less trustworthy and spur higher consumer security behavior compared to companies that have not been breached, was partially supported. Specifically, we found that individuals reported more trust in companies when they had never been breached. However, participants did not create more complex passwords or indicate more security engagement in response to known data breaches. This interesting result was contrary to our predictions. Our second hypothesis, which related to the manipulation of the confidence of the security statements, was not supported.

It appears that even contradictory information (i.e. overconfidence + the presence of a breach) does not seem to motivate participants towards the behavioral intention of a more complex password. Further, there is no evidence that overconfident companies suffer much in the way of detrimental trust effects, as compared to realistic or underconfident companies when they have the presence of a breach. Further, we expected that the confidence projected in a company security statement would influence perceptions of trust and intended user security behavior, and there is some evidence to support our results. Specifically, Belanger *et al.* (2002) found that trust in a company is more generally determined first by the pleasure features of online use, then by the perceived security features and rarely by security statements themselves. Further, Metzger (2006) found that consumer trust is more strongly influenced by reputation rather than the framing of security assurances. Thus, this study provides further support that company statements are less important than perhaps previously considered when it comes to trusting a company.

These findings point towards two major issues in consumer psychology. First, given that we are all vulnerable to attacks, consumers seem less concerned with what *will* happen as much as they are concerned with what *has* happened. To the degree that past behavior is predictive of future behavior, this is a fair assumption. However, it may also be the case that

Table IV.
Cell counts for a two-way contingency table of breach and company choice

		Observed		Expected	
Breach	Company	Count	(%)	Count	(%)
Absent	Overconfident	60	25.4	55.93	23.7
	Realistic	57	24.2	56.95	24.1
	Under confident	3	1.3	7.12	3.0
Present	Overconfident	50	21.2	54.07	22.9
	Realistic	55	23.3	55.05	23.3
	Under confident	11	4.7	6.88	2.9

companies that have been breached are especially secure and have made great strides following a breach to tighten their online security. Thus, these companies may be among the safest and most trustworthy. However, it appears, at least from the data available, that consumers perceive them as less so.

Perhaps more interesting and concerning is the finding that, although a security breach lowers consumer trust, it seems to have no impact on the behavioral intentions of consumers to be secure. We found no evidence that intended password strength varied as a function of security statement strength or breach status. This finding adds further evidence to the idea that consumers do not feel that they are responsible for their own security when logging onto an established company's website. Even when that company had been breached, individuals do not tighten their own security.

There are a few potential explanations for this lack of behavioral change. The first is that consumers feel that it is the company's job to secure private information. The second is that they feel that breaches are rare and the effort put forth to generate and retain in memory a complex password is not worth the effort commensurate with the probability of the event occurring. A third explanation is learned helplessness (Abramson *et al.*, 1978). Individuals may feel that what goes on with respect to security breaches is beyond their control, and nothing they (personally) do will help prevent an attack or data leaks. Future research would benefit from further study and direct comparisons of these three possibilities. The research underlying the lack of security motivation by consumers could contribute to efforts and applications to convince users to protect themselves by actively engaging in more secure behaviors. By understanding why consumers do not want to generate more complex passwords in breached or uncertain security environments, we stand a greater chance of fighting those reasons in the service of greater online security.

In sum, online security is of great concern and companies that have had a breach face reputational damage. Our findings further assert that this damage emerges regardless of how confident companies express themselves through security statements. Further, consumers do not seem likely to change their password strength regardless of company confidence or the presence of a breach.

References

Abramson, L.Y., Seligman, M.E. and Teasdale, J.D. (1978), "Learned helplessness in humans: critique and reformulation", *Journal of Abnormal Psychology*, Vol. 87 No. 1, pp. 49-74.

Acquisti, A., Friedman, A. and Telang, R. (2006), "Is there a cost to privacy breaches? An event study", *ICIS 2006 Proceedings*, p. 94.

Belanger, F., Hiller, J.S. and Smith, W.J. (2002), "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes", *The Journal of Strategic Information Systems*, Vol. 11 No. 3, pp. 245-270.

Berendt, B., Günther, O. and Spiekermann, S. (2005), "Privacy in e-commerce: stated preferences vs actual behavior", *Communications of the ACM*, Vol. 48 No. 4, pp. 101-106.

Berezina, K., Cobanoglu, C., Miller, B.L. and Kwansa, F.A. (2012), "The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth", *International Journal of Contemporary Hospitality Management*, Vol. 24 No. 7, pp. 991-1010.

Buhrmester, M., Kwang, T. and Gosling, S.D. (2011), "Amazon's mechanical Turk: a new source of inexpensive, yet high-quality, data?", *Perspectives on Psychological Science*, Vol. 6 No. 1, pp. 3-5.

Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003), "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", *Journal of Computer Security*, Vol. 11 No. 3, pp. 431-448.

Carré, J.R., Curtis, S.R. and Jones, D.N. (2018), "Ascribing responsibility for online security and data breaches", *Managerial Auditing Journal*.

Cazier, J.A. and Medlin, B.D. (2006), "Password security: an empirical investigation into e-commerce passwords and their crack times", *Information Systems Security*, Vol. 15 No. 6, pp. 45-55.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S. and Rao, H.R. (2016), "Online shopping intention in the context of data breach in online retail stores: an examination of older and younger adults", *Decision Support Systems*, Vol. 83, pp. 47-56.

Curtis, S.R., Rajivan, P., Jones, D.N. and Gonzalez, C. (2017), "Phishing attempts among the Dark Triad: patterns of attack and vulnerability", *Manuscript Under Review*.

de Carnavalet, X.D.C. and Mannan, M. (2014), "From very weak to very strong: analyzing password-strength meters", *Network and Distributed System Security (NDSS)*, Vol. 14, pp. 23-26.

Egelman, S. and Peer, E. (2015), "Scaling the security wall: developing a security behavior intentions scale (sebis)", *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, ACM*, pp. 2873-2882.

Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K. and Herley, C. (2013), "Does my password go up to eleven? The impact of password meters on password selection", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM*, pp. 2379-2388.

Garg, A., Curtis, J. and Halper, H. (2003), "Quantifying the financial impact of IT security breaches", *Information Management & Computer Security*, Vol. 11 No. 2, pp. 74-83.

Ives, B., Walsh, K.R. and Schneider, H. (2004), "The domino effect of password reuse", *Communications of the ACM*, Vol. 47 No. 4, pp. 75-78.

Kang, R., Dabbish, L., Fruchter, N. and Kiesler, S. (2015), "'My data just goes everywhere': user mental models of the internet and implications for privacy and security", *Symposium on Usable Privacy and Security (SOUPS), USENIX Association, Berkeley, CA*, pp. 39-52.

Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F. and Lopez, J. (2012), "Guess again (and again and again): measuring password strength by simulating password-cracking algorithms", *2012 IEEE Symposium on Security and Privacy (SP), IEEE*, pp. 523-537.

Kim, C., Tao, W., Shin, N. and Kim, K.S. (2010), "An empirical study of customers' perceptions of security and trust in e-payment systems", *Electronic Commerce Research and Applications*, Vol. 9 No. 1, pp. 84-95.

Knowles, E.S. and Riner, D.D. (2007), "Omega approaches to persuasion: overcoming resistance", *The Science of Social Influence: Advances and Future Progress*, pp. 83-114.

Metzger, M.J. (2006), "Effects of site, vendor, and consumer characteristics on web site trust and disclosure", *Communication Research*, Vol. 33 No. 3, pp. 155-179.

Miyazaki, A.D. and Fernandez, A. (2001), "Consumer perceptions of privacy and security risks for online shopping", *Journal of Consumer Affairs*, Vol. 35 No. 1, pp. 27-44.

Morse, E.A., Raval, V. and Wingender, J.R. Jr (2011), "Market price effects of data security breaches", *Information Security Journal: A Global Perspective*, Vol. 20 No. 6, pp. 263-273.

Ng, B.Y., Kankanhalli, A. and Xu, Y.C. (2009), "Studying users' computer security behavior: a health belief perspective", *Decision Support Systems*, Vol. 46 No. 4, pp. 815-825.

Papacharissi, Z. and Fernback, J. (2005), "Online privacy and consumer protection: an analysis of portal privacy statements", *Journal of Broadcasting & Electronic Media*, Vol. 49 No. 3, pp. 259-281.

Proctor, R.W., Lien, M.C., Vu, K.P.L., Schultz, E.E. and Salvendy, G. (2002), "Improving computer security for authentication of users: influence of proactive password restrictions", *Behavior Research Methods*, Vol. 34 No. 2, pp. 163-169.

Schneier, B. (2011), *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons.

Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N. and Cranor, L.F. (2010), "Encountering stronger password requirements: user attitudes and behaviors", *Proceedings of the Sixth Symposium on Usable Privacy and Security, ACM*, p. 2.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005), "Analysis of end user security behaviors", *Computers & Security*, Vol. 24 No. 2, pp. 124-133.

Summers, W.C. and Bosworth, E. (2004), "Password policy: the good, the bad, and the ugly", *Proceedings of the Winter International Symposium on Information and Communication Technologies, Trinity College Dublin*, pp. 1-6.

Ur, B., Kelley, P.G., Komanduri, S., Lee, J., Maass, M., Mazurek, M.L., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N. and Cranor, L.F. (2012), "How does your password measure up? The effect of strength meters on password creation", *USENIX Security Symposium*, pp. 65-80.

Weir, M., Aggarwal, S., Collins, M. and Stern, H. (2010), "Testing metrics for password creation policies by attacking large sets of revealed passwords", *Proceedings of the 17th ACM Conference on Computer and Communications Security, ACM*, pp. 162-175.

Zviran, M. and Haga, W.J. (1999), "Password security: an empirical study", *Journal of Management Information Systems*, Vol. 15 No. 4, pp. 161-185.

Further reading

Hong, J. (2012), "The state of phishing attacks", *Communications of the ACM*, Vol. 55 No. 1, pp. 74-81.

About the authors

Shelby R. Curtis is a PhD Student in her third year in the Department of Psychology at the University of Texas at El Paso.

Jessica Rose Carre is a PhD Student in her final year in the Department of Psychology at the University of Texas at El Paso.

Daniel Nelson Jones is an Assistant Professor in the Department of Psychology at the University of Texas at El Paso. Daniel Nelson Jones is the corresponding author and can be contacted at: jonesdn@gmail.com